



Manual Prático da LGPD

Hospital Cantinho do Céu



CANTINHO DO CÉU
HOSPITAL DE RETAGUARDA



Boas-vindas



Seja bem-vindo (a) ao nosso hospital.

Sabemos que confiar o cuidado de quem você ama a uma instituição de saúde exige segurança, acolhimento e respeito,

No **Hospital Cantinho do Céu**, o cuidado é contínuo, atento e centrado na dignidade, no conforto e na qualidade de vida do paciente.

Esta cartilha foi elaborada para orientar os colaboradores sobre a LGPD no ambiente hospitalar, fortalecendo a proteção de dados dos pacientes e contribuindo para um ambiente seguro, ético e responsável.

Introdução: Por que a LGPD é importante para você e para o Hospital Cantinho do Céu?

Este manual foi criado para ajudar você a entender a **Lei Geral de Proteção de Dados Pessoais (LGPD)** e como ela se aplica ao seu dia a dia aqui no **Hospital Cantinho do Céu**.

Sabemos que o ambiente hospitalar lida com informações muito sensíveis, e a proteção desses dados é fundamental para a confiança dos nossos pacientes e para a segurança da nossa instituição.

A **LGPD** é uma lei brasileira que protege a privacidade e os direitos das pessoas em relação aos seus dados pessoais. Ela exige que todas as empresas e instituições, incluindo hospitais, tratem os dados de forma responsável, transparente e segura. Para nós, no **Cantinho do Céu**, que cuidamos de pacientes com necessidades especiais e suas famílias, essa responsabilidade é ainda maior.

Seu papel é essencial!

Cada um de nós, ao lidar com informações de pacientes, familiares, fornecedores ou colegas, é um guardião desses dados. Entender e aplicar a **LGPD** não é apenas uma obrigação legal, mas um compromisso com a ética, o respeito e a qualidade do nosso trabalho.

Este manual é um guia prático. Ele vai explicar:

- O que é a **LGPD** e seus princípios básicos.
- Quais dados são protegidos.
- O que você pode e não pode fazer com os dados.
- Como agir no dia a dia para proteger as informações.
- O que fazer em caso de dúvidas ou incidentes.

Vamos juntos garantir que o **Hospital Cantinho do Céu** continue sendo um ambiente seguro e confiável para todos!

1. O que é a LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, é a legislação brasileira que regula como as informações pessoais devem ser coletadas, usadas, armazenadas e compartilhadas. Ela foi criada para proteger a privacidade e a liberdade das pessoas, dando a elas mais controle sobre seus próprios dados. Pense assim: Seus dados pessoais são como seus pertences mais valiosos. A **LGPD** é a lei que garante que ninguém use seus pertences sem sua permissão ou de forma inadequada. Isso vale para os dados dos nossos pacientes e de todos com quem nos relacionamos.

Quem a LGPD protege?

A **LGPD** protege os dados pessoais de pessoas físicas (indivíduos), sejam eles pacientes, acompanhantes, visitantes, funcionários, fornecedores ou qualquer outra pessoa que tenha seus dados tratados pelo hospital.

Onde a LGPD se aplica?

A **LGPD** se aplica a qualquer operação de tratamento de dados pessoais realizada no Brasil ou que envolva dados de pessoas localizadas no Brasil, mesmo que a empresa esteja em outro país. Ou seja, ela se aplica diretamente a todas as atividades do **Hospital Cantinho do Céu**.



2. Princípios Fundamentais da LGPD

Para entender a **LGPD**, é importante conhecer os princípios que a norteiam. Eles são a base para todas as nossas ações e decisões ao lidar com dados pessoais:

- **Finalidade:** Os dados devem ser coletados para propósitos legítimos, específicos, explícitos e informados ao titular. Não podemos coletar dados sem um motivo claro e sem informar a pessoa sobre esse motivo.

Exemplo: Coletar o nome e CPF de um paciente para o cadastro hospitalar e emissão de nota fiscal é uma finalidade legítima. Coletar a religião do paciente sem um motivo médico ou assistencial claro não seria.

- **Adequação:** O tratamento dos dados deve ser compatível com as finalidades informadas. Não podemos usar os dados para algo diferente do que foi dito inicialmente.

Exemplo: Usar o endereço do paciente para enviar correspondências relacionadas ao tratamento é adequado. Usar o mesmo endereço para enviar publicidade de produtos não relacionados à saúde, sem consentimento, não seria adequado.

- **Necessidade:** Devemos coletar e tratar apenas os dados estritamente necessários para atingir a finalidade. Evite coletar informações excessivas.

Exemplo: Para agendamento de consulta, o nome completo e telefone são necessários. Perguntar sobre a renda familiar, sem um contexto assistencial específico e justificado, seria excessivo.

- **Livre Acesso:** O titular dos dados tem o direito de acessar suas informações de forma facilitada e gratuita.

Exemplo: Um paciente pode solicitar uma cópia de seu prontuário médico a qualquer momento, e o hospital deve fornecer essa informação de maneira clara e sem custos.



- **Qualidade dos Dados:** Os dados devem ser exatos, claros, relevantes e atualizados.

Exemplo: É importante manter os cadastros dos pacientes atualizados, com informações de contato corretas e histórico médico preciso.

- **Transparência:** As informações sobre o tratamento dos dados devem ser claras, precisas e facilmente acessíveis.

Exemplo: O hospital deve ter uma política de privacidade de fácil acesso, explicando como os dados são tratados.

- **Segurança:** Medidas técnicas e administrativas devem ser adotadas para proteger os dados de acessos não autorizados, destruição, perda, alteração ou qualquer forma de tratamento inadequado.

Exemplo: Senhas fortes, sistemas protegidos, e cuidado ao manusear prontuários físicos são exemplos de medidas de segurança.

- **Prevenção:** Devemos agir para prevenir a ocorrência de danos em virtude do tratamento de dados.

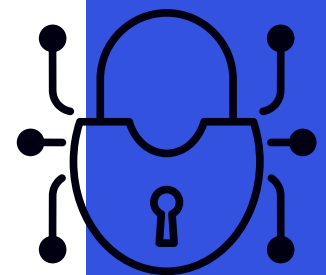
Exemplo: Treinamentos regulares sobre LGPD e segurança da informação ajudam a prevenir incidentes.

- **Não Discriminação:** O tratamento de dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos.

Exemplo: Não podemos usar informações de saúde de um paciente para negar-lhe um serviço ou tratamento, a menos que haja uma justificativa médica clara e ética.

- **Responsabilização e Prestação de Contas:** O hospital deve demonstrar a adoção de medidas eficazes para o cumprimento da LGPD e a proteção dos dados.

Exemplo: Manter registros de como os dados são tratados, quem tem acesso e quais medidas de segurança estão em vigor.



3. Dados Pessoais e Dados Pessoais Sensíveis: Qual a diferença?

A **LGPD** faz uma distinção importante entre dados pessoais comuns e dados pessoais sensíveis, pois estes últimos exigem um nível ainda maior de proteção.



3.1. Dados Pessoais

São informações que podem identificar uma pessoa, direta ou indiretamente.

Exemplos:

- Nome completo
- CPF, RG
- Endereço
- Telefone
- E-mail
- Data de nascimento
- Número do prontuário
- Placa do carro
- Endereço IP



3.2. Dados Pessoais Sensíveis

São dados que revelam aspectos mais íntimos e que, se tratados de forma inadequada, podem gerar discriminação ou prejuízos significativos ao titular.

No contexto hospitalar, são exemplos cruciais:

- Dados referentes à saúde: Histórico médico, resultados de exames, diagnósticos, tratamentos, informações sobre doenças, deficiências (como a paralisia cerebral dos nossos pacientes).
- Dados genéticos: Informações sobre o DNA de uma pessoa.
- Dados biométricos: Impressões digitais, reconhecimento facial.
- Origem racial ou étnica
- Convicção religiosa
- Opinião política
- Filiação a sindicato ou a organização de caráter religioso, filosófico ou político
- Vida sexual



Atenção: O tratamento de dados pessoais sensíveis, especialmente os de saúde, requer consentimento específico e destacado do titular ou de seu responsável legal, salvo exceções previstas em lei (como para a tutela da saúde, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária).

4. O que podemos fazer com os dados? (E o que não podemos!) ✓ ✗

Para garantir a conformidade com a **LGPD** e proteger nossos pacientes, é fundamental saber o que é permitido e o que é proibido no tratamento de dados.

Lembre-se: todo dado pessoal pertence ao titular, não ao hospital ou ao funcionário.



4.1. O que PODEMOS fazer (com responsabilidade e base legal):

Ação permitida	Explicação e Exemplo	Base Legal Comum	Observações
Coletar dados necessários	Obter informações essenciais para o atendimento, cadastro e tratamento do paciente. <i>Exemplo: Coletar nome, CPF, histórico médico e exames para o prontuário.</i>	Consentimento do titular ou Tutela da Saúde	Apenas o mínimo necessário para a finalidade.
Utilizar dados para o tratamento	Acessar e usar as informações do paciente para diagnóstico, tratamento, acompanhamento e procedimentos médicos. <i>Exemplo: O médico acessa o prontuário para prescrever medicamentos.</i>	Tutela da Saúde	Acesso restrito aos profissionais envolvidos no cuidado.
Compartilhar dados internamente	Trocar informações entre a equipe multidisciplinar (médicos, enfermeiros, fisioterapeutas, etc.) para garantir o cuidado integral do paciente. <i>Exemplo: A equipe de enfermagem informa ao fisioterapeuta sobre a condição de mobilidade do paciente.</i>	Tutela da Saúde	Apenas com quem precisa saber para o cuidado do paciente.

Ação permitida	Explicação e Exemplo	Base Legal Comum	Observações
Compartilhar dados com terceiros (com cautela)	Em casos específicos e com base legal, como com convênios médicos, laboratórios parceiros ou autoridades de saúde. <i>Exemplo: Enviar resultados de exames para o laboratório que os realizou.</i>	Cumprimento de obrigação legal ou Tutela da Saúde	Sempre com contratos que garantam a proteção dos dados.
Armazenar dados de forma segura	Manter prontuários físicos em locais trancados e sistemas digitais protegidos por senhas e criptografia. <i>Exemplo: Guardar prontuários em armários com chave e sistemas com acesso restrito.</i>	Cumprimento de obrigação legal	Por tempo determinado pela legislação.
Informar o titular sobre o tratamento	Explicar ao paciente ou responsável como seus dados serão usados, por que e por quanto tempo. Exemplo: Apresentar a política de privacidade e obter o consentimento informado.	Transparência	Essencial para a confiança e o direito do titular.



4.2. O que NÃO PODEMOS fazer (e as consequências):

Ação proibida	Explicação e Exemplo	Consequências
Coletar dados desnecessários	Pedir informações que não são relevantes para a finalidade do atendimento ou serviço. <i>Exemplo: Perguntar sobre a vida pessoal do paciente que não tem relação com seu tratamento.</i>	Violação do princípio da necessidade.
Filmar, fotografar ou gravar sem consentimento	Registrar imagens ou voz de pacientes, acompanhantes ou colegas sem autorização expressa. <i>Exemplo: Tirar uma foto de um paciente no leito para mostrar a um amigo.</i>	Violação da privacidade, processo judicial, demissão por justa causa.
Compartilhar dados sem base legal (vazar)	Divulgar informações de pacientes, mesmo que para colegas que não estão envolvidos no tratamento, ou para pessoas externas. <i>Exemplo: Comentar sobre o diagnóstico de um paciente com um amigo ou familiar que não é o responsável legal.</i>	Violação de sigilo profissional, processo judicial, demissão por justa causa, multas para o hospital.



Ação proibida	Explicação e Exemplo	Consequências
Acessar dados sem necessidade	Consultar prontuários ou sistemas de informação de pacientes que não estão sob sua responsabilidade direta. <i>Exemplo: Um funcionário da recepção acessa o prontuário de um paciente por curiosidade.</i>	Violação do princípio do mínimo privilégio, processo judicial, demissão por justa causa.
Deixar documentos com dados expostos	Abandonar prontuários, exames ou qualquer documento com informações pessoais em locais de fácil acesso ou visíveis a terceiros. <i>Exemplo: Deixar um prontuário aberto na mesa da recepção ou em um balcão.</i>	Risco de vazamento de dados, violação da segurança.
Usar redes sociais para discutir casos	Postar ou comentar sobre pacientes, mesmo que de forma indireta ou sem identificação, em redes sociais ou grupos de mensagens. <i>Exemplo: Publicar no Facebook sobre um caso interessante que atendeu no hospital.</i>	Violação de sigilo profissional, processo judicial, demissão por justa causa.
Descartar dados de forma inadequada	Jogar no lixo comum documentos com informações pessoais sem triturar ou inutilizar. <i>Exemplo: Descartar uma ficha de paciente diretamente na lixeira.</i>	Risco de vazamento de dados, violação da segurança.

5. Como agir no dia a dia: Exemplos Práticos

Para que a **LGPD** faça parte da nossa rotina, veja alguns exemplos de como você deve agir em situações comuns:



Situação 1: Um familiar pergunta sobre o estado de saúde de um paciente.

O que fazer: Verifique se o familiar está autorizado a receber informações (cadastro no prontuário, consentimento do paciente). Se sim, forneça apenas as informações estritamente necessárias e autorizadas. Se não, informe que, por questões de privacidade e sigilo, você não pode fornecer detalhes.

O que não fazer: Fornecer informações a qualquer pessoa que se diga familiar sem verificar a autorização. Comentar sobre o estado do paciente em corredores ou áreas comuns onde outras pessoas possam ouvir.

Situação 2: Você encontra um prontuário ou documento com dados de paciente em um local inadequado.



O que fazer: Recolha imediatamente o documento e entregue-o ao seu superior ou à área responsável pela guarda de prontuários. Informe o ocorrido para que as medidas cabíveis sejam tomadas.

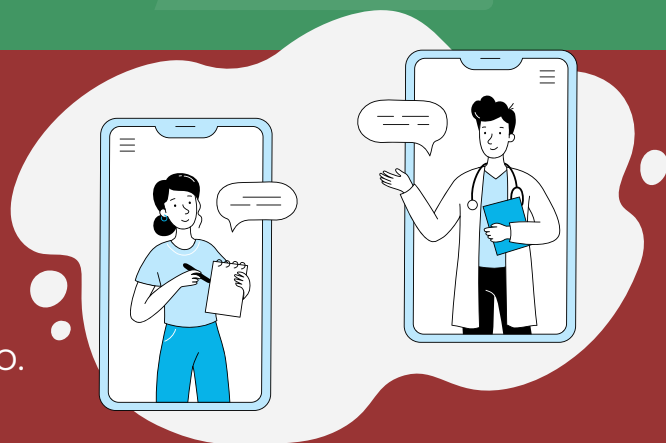
O que não fazer: Ignorar o documento. Ler o conteúdo por curiosidade. Deixar o documento onde está.

Situação 3: Você precisa enviar informações de um paciente para outro setor ou profissional.

O que fazer: Utilize os canais de comunicação internos e seguros do hospital (sistemas específicos, e-mail corporativo criptografado). Certifique-se de que o destinatário é o profissional correto e que ele tem necessidade de acesso àquela informação para o tratamento do paciente.



O que não fazer: Enviar informações por e-mail pessoal, WhatsApp ou outros meios não seguros. Enviar dados para um profissional que não está diretamente envolvido no caso.



Situação 4: Um paciente solicita acesso ao seu prontuário.

O que fazer: Oriente o paciente sobre o procedimento para solicitação de acesso ao prontuário, que geralmente envolve um pedido formal à área responsável. O hospital tem um prazo para atender a essa solicitação.

O que não fazer: Negar o acesso sem justificativa legal. Dificultar o processo de solicitação.

Situação 5: Você percebe uma atividade suspeita em um sistema ou com dados de pacientes.

O que fazer: Comunique imediatamente seu superior e/ou o Encarregado de Dados (DPO) do hospital. Descreva o que você observou com o máximo de detalhes possível.

O que não fazer: Tentar resolver a situação sozinho. Ignorar a situação. Comentar com colegas que não são da equipe responsável.



6. O Encarregado de Dados (DPO) e o Comitê de Proteção de Dados

O Hospital Cantinho do Céu possui um Encarregado de Dados (DPO - Data Protection Officer) e um Comitê de Proteção de Dados. Eles são as figuras centrais para a conformidade com a LGPD na nossa instituição.



6.1. Encarregado de Dados (DPO)

O **DPO** é a pessoa responsável por:

- Atuar como canal de comunicação entre o hospital, os titulares dos dados (pacientes, funcionários, etc.) e a Autoridade Nacional de Proteção de Dados (ANPD).
- Orientar os funcionários e o hospital sobre as práticas de proteção de dados.
- Receber reclamações e comunicações dos titulares, prestando esclarecimentos e adotando providências.
- Receber comunicações da ANPD e adotar providências.



*Em caso de dúvidas sobre a **LGPD** ou qualquer situação envolvendo dados pessoais, o **DPO** é a sua principal referência!*



6.2. Comitê de Proteção de Dados

É um grupo multidisciplinar que auxilia o **DPO** e a direção do hospital na implementação e monitoramento das políticas de proteção de dados, garantindo que a **LGPD** seja aplicada em todas as áreas da instituição.



7. O que acontece se a lei for descumprida?

O descumprimento da **LGPD** pode trazer sérias consequências, tanto para o funcionário quanto para o **Hospital Cantinho do Céu**.



Para o funcionário:

- Processo judicial de caráter trabalhista: Pode levar à demissão por justa causa.
- Processo civil e criminal: Dependendo da gravidade do vazamento ou uso indevido dos dados.
- Dano moral e material: Responsabilidade por eventuais prejuízos causados aos titulares dos dados.

Para o Hospital Cantinho do Céu:

- **Advertências e multas:** A ANPD pode aplicar multas que variam de 2% do faturamento da empresa (limitado a R\$ 50 milhões por infração) até a suspensão das atividades de tratamento de dados.
- **Suspensão das atividades:** Em casos extremos, o hospital pode ter suas atividades de tratamento de dados suspensas.
- **Dano à reputação:** Perda de confiança dos pacientes e da comunidade, o que pode afetar a imagem e a sustentabilidade da instituição.
- **Obrigatoriedade de publicizar a infração:** A ANPD pode determinar a publicização da infração, expondo o hospital.

A proteção de dados é uma responsabilidade de todos. Agir com ética e cuidado é fundamental para evitar essas consequências.

Conclusão:

Parabéns por chegar até aqui! Agora você tem um conhecimento mais aprofundado sobre a **LGPD** e a importância da proteção de dados no **Hospital Cantinho do Céu**. Lembre-se que este manual é um guia, e a legislação pode ter atualizações. Mantenha-se sempre atento e, em caso de dúvidas, procure o Encarregado de Dados (DPO) ou seu superior.



Sua colaboração é vital para garantirmos um ambiente seguro e de confiança para nossos pacientes e para toda a comunidade do **Cantinho do Céu**. **Contamos com você!**



CANTINHO DO CÉU
HOSPITAL DE RETAGUARDA

   [cantinhodoceurp](#)

 **(16) 3622-0853**

www.cantinhodoceurp.org.br

Rua Rio Verde, 357 | Ipiranga | Ribeirão Preto-SP
